Legislative Assembly of Ontario

Assemblée législative de l'Ontario

Official Report of Debates (Hansard)

P-12

Standing Committee on Public Accounts

2016 Annual Report, Auditor General:

Treasury Board Secretariat

2nd Session
41st Parliament

Wednesday 31 May 2017

Chair: Ernie Hardeman
Clerk: Katch Koch

Journal des débats (Hansard)

P-12

Comité permanent des comptes publics

Rapport annuel 2016, vérificatrice générale :

Secrétariat du Conseil du Trésor

2e session
41e législature

Mercredi 31 mai 2017

Président : Ernie Hardeman
Greffier : Katch Koch

Hansard on the Internet

Hansard and other documents of the Legislative Assembly can be on your personal computer within hours after each sitting. The address is:

Le Journal des débats sur Internet

L'adresse pour faire paraître sur votre ordinateur personnel le Journal et d'autres documents de l'Assemblée législative en quelques heures seulement après la séance est :

http://www.ontla.on.ca/

Index inquiries

Reference to a cumulative index of previous issues may be obtained by calling the Hansard Reporting Service indexing staff at 416-325-7400.

Renseignements sur l'index

Adressez vos questions portant sur des numéros précédents du Journal des débats au personnel de l'index, qui vous fourniront des références aux pages dans l'index cumulatif, en composant le 416-325-7400.

Hansard Reporting and Interpretation Services
Room 500, West Wing, Legislative Building
111 Wellesley Street West, Queen's Park
Toronto ON M7A 1A2
Telephone 416-325-7400; fax 416-325-7430
Published by the Legislative Assembly of Ontario

ISSN 1180-4327

Service du Journal des débats et d'interprétation
Salle 500, aile ouest, Édifice du Parlement
111, rue Wellesley ouest, Queen's Park
Toronto ON M7A 1A2
Téléphone, 416-325-7400; télécopieur, 416-325-7430
Publié par l'Assemblée législative de l'Ontario

CONTENTS

Wednesday 31 May 2017

2016 Annual Report, Auditor General.....P-195
Treasury Board Secretariat.....P-195
Ms. Helen Angus
Mr. David Nicholl
Ms. Robin Thompson
Mr. Mohammad Qureshi
Ms. Wynnann Rose

LEGISLATIVE ASSEMBLY OF ONTARIO

STANDING COMMITTEE ON PUBLIC ACCOUNTS

Wednesday 31 May 2017

ASSEMBLÉE LÉGISLATIVE DE L'ONTARIO

COMITÉ PERMANENT DES COMPTES PUBLICS

Mercredi 31 mai 2017

The committee met at 1232 in room 151, following a closed session.

2016 ANNUAL REPORT, AUDITOR GENERAL

TREASURY BOARD SECRETARIAT

Consideration of section 4.03, information and information technology general controls.

The Chair (Mr. Ernie Hardeman): The time has arrived. We'll call the meeting of the public accounts committee to order. We're here this afternoon to review section 4.03 of the 2016 Annual Report of the Office of the Auditor General of Ontario. This afternoon we're hearing delegations from the Treasury Board Secretariat and Helen Angus, deputy minister. Welcome. Thank you very much for being here.

As we normally do, we will provide a 20-minute opportunity for the deputants to make a presentation. If more than one person is going to speak, we would ask each one to introduce themselves as they speak for the first time so that we can get the proper name and identification for the Hansard.

With that, you will have 20 minutes, and then at the end of 20 minutes, we will start the rotation of the three caucuses with a 20-minute rotation to ask questions and comments. We will start this rotation with the government side.

At the end of that, we will then take the time that is left that will take us to 2:45, which we will divide three ways, and we will go one more time around to finish the afternoon. Again, we will start off by giving you the 20 minutes. Thank you, again, for being here this afternoon.

Ms. Helen Angus: Thank you very much. It's a great pleasure, and it sounds like a good plan.

I'm really pleased to have the opportunity to address the Standing Committee on Public Accounts. First off, I'd like to thank the Auditor General and her team for the recommendations on IT general controls. They did a very thorough job. I hope you'll see, through the presentation that I will give, as well as David Nicholl, who is on my left here, how seriously we've taken those recommendations and how we're moving forward on implementation.

I must say, I was pleased to see that the Auditor General noted in her report that the I&IT management is moving in the right direction when it comes to the backup, recovery and operation of I&IT general controls. I very much believe that to be the case, and the guidance provided by the Auditor General has been very instructive in taking our work further.

We've been working very hard over the ensuing months since the audit to address the recommendations. I believe that we're making very good progress, but there is still room for improvement, so there is still work for us to do.

I'm joined, as I mentioned earlier, by David Nicholl, who is our corporate chief information officer. You may have seen him at public accounts before. So here is David.

We have a number of other colleagues who might be able to answer specific questions that you have: Robin Thompson, Wynnann Rose and Ron Huxter, who are over here, who are the chief information officers responsible for the systems that are examined in the audit. We also have here with us Mohammad Qureshi, who is the lead of our cybersecurity operations, in case there are any questions related to that.

For us, IT is not just about systems and controls, which are incredibly important, but it's a whole lot more than that. The IT organization plays a huge role in the government's transformation journey and is a key part of the Treasury Board Secretariat, which leads the government's efforts on accountability, openness and modernization. Like its parent, the Treasury Board Secretariat, the IT organization strives to continuously improve. It is the backbone for delivering excellent government services in the most effective and efficient way possible. It also provides the Ontario government with business solutions that support ministry priorities as well as strategic advice and leadership on the use of IT. And it ensures the security and integrity of all our systems and networks. I hope that gives you an overview of what the function is.

It also enables the provision of modern and efficient services for the public and helps uphold the government's responsibility to protect privacy and encourage transparency.

This organization, which David leads, is responsible for all the IT infrastructure systems and support for the province. Just to give you a sense of the scope, which I think was well documented in the Auditor General's report, it includes about 1,200 applications that help ministries deliver critical services to Ontarians. To give you an example of that, that would include social assistance and child welfare systems, driver's licensing,

health cards and other ServiceOntario transactions, and emergency response services. The scope of the operation is really considerable.

To get a sense of the numbers: nine million drivers and 11 million vehicles are in the Ministry of Transportation's database; eight million social assistance payments to more than 900,000 recipients are processed monthly; and nearly 200 million Ontario drug benefit claims are processed annually.

This just gives you a sample of the scope of the IT organization's work. There certainly is room to improve, and I think the audit recommendations have been a valuable tool to help us enhance our efforts with respect to the continuous improvement of our IT systems and delivery.

I'll ask David to walk through, in a little bit more detail, as a jumping-off point for the questions that you may have, an update on the progress that we've made on the audit recommendations, because I think that's relevant to the interests of the committee.

David, can you take it from there? Give an overview, please.

Mr. David Nicholl: Absolutely. I'm David Nicholl, corporate chief information officer for the Ontario government from Treasury Board Secretariat. Thank you, Deputy Angus.

As noted, the auditor provided really valuable insights into our efforts to improve the integrity of our systems with respect to IT general controls. I have to say that the audit team were great to work with. I'm sure you don't hear that all the time, but it's certainly true in this case. We really do appreciate very much the observations and the recommendations. The Auditor General and I met previous to the audit, and I made it really clear that this was a very important part of our process that we were going through, and to get the kind of independent advice from a body like them was just what we needed. And it's the way it worked out.

Like the deputy, clearly, I'm totally committed to addressing the audit, but it's far, far more than that for us. It's much more than just addressing a bunch of "tick the boxes" from an audit perspective. It's much more around really taking us to the next level from a performance perspective.

Regarding service management, the auditor specifically noted the real importance of having what we call service-level agreements, or SLAs for short. She recommended the establishment of formal SLAs as part of having effective IT general controls.

Service management is really critical to ensuring high-quality services that meet the needs of the government and the citizens of Ontario. Service management is the behind-the-scenes work that supports ministry applications and their services to the public, whether it's implementing new applications, changing those applications, or, in the very occasional times we have some issues, fixing those issues.

It also includes our internal customer interface for IT products and services like our helpdesk or our service order desk.

1240

We understand and agree completely that consistent and enterprise-wide SLAs are necessary to monitor and report back on service effectiveness, and ensure our system integrity.

Our approach to service management is robust. Over time, we've leveraged best practices and evidence. We've continually assessed and matured, all the while ensuring service continuity. Previous to last year, we were very focused on our infrastructure service management piece, when we consolidated service management back in 2008-09 for infrastructure. We focused very much on the formal portions of SLAs between infrastructure and cluster, and I think probably around 2014 we realized that we had a gap, from a formality perspective, between cluster to ministry. In October 2016, we established a new Enterprise Service Management division, or eSM. The division brings together practitioners from across the IT organization, specifically our clusters, to uniformly deliver services across the enterprise—so very much a similar exercise as to what we had done previously with infrastructure, we're now replicating within the cluster/ministry model.

Service management under one division will certainly improve our internal IT service delivery and find some efficiencies, but more importantly, it will enable consistent processes and service levels across the whole organization—so not cluster by cluster, but actually a consistent approach no matter what ministry, what cluster.

A real focus for the division is addressing the improvements regarding SLAs, in line with the audit recommendations. In fact, establishing an eSM organization to implement SLAs across the government responds very specifically to the auditor's recommendations to ensure that we are delivering high-quality and consistent services that meet the needs of the ministries.

While some agreements have been in place between clusters and client ministries in the past, what eSM is really doing is formalizing those agreements with a consistent, enterprise-wide approach. This approach includes all nine SLA elements identified by the Auditor General.

The eSM division is still relatively new. However, we have already undertaken significant work to enable greater consistency in SLAs across all clusters. We have established an enterprise-wide governance model and are working to establish a government of Ontario IT standard for service-level management. This will ensure SLAs are in place between all clusters and ministries.

We're also working to expand the scope of existing SLAs to more closely align with our current IT strategy, as per the auditor's recommendation. This will include things like performance metrics for mission- and business-critical applications. To ensure regular reporting, we are developing an SLA reporting framework and template. To support these activities, the eSM team will

be providing training and communications materials to our IT clusters and ministry partners.

The eSM division is providing leadership and guidance on SLAs and is responsible for establishing and maturing processes to ensure these important agreements are in place.

To ensure the continuous improvement with service management, we will continue working with our HR partners and the Centre for Leadership and Learning to focus on skills development and succession planning. We take this work very seriously, and we continue to make steady progress for the eSM division.

The auditor noted the age of some of our applications. Specifically, she cited the need to replace and modernize, where possible, and to have appropriate strategies in place to ensure appropriate maintenance and support, to mitigate issues with systems performance. I totally agree with this. I recognize the value in having a comprehensive inventory, life-cycle management and planning approach in place to ensure appropriate systems maintenance and replacement.

There are potential risks associated with older applications, and it's imperative that we maintain applications properly in order to protect public services, but as noted in the audit, the age of the system in itself is not necessarily the issue. Age does not equal risk. That said, the IT organization's modernization approach to applications has been in place for just over a decade, and it continues to evolve. Assessments were undertaken in 2006 and 2007, and a baseline for tracking major applications was established in 2008. This informed what we call our Major Applications Portfolio Strategy, or MAPS. As well, it identified 77 major applications requiring immediate attention. Six hundred million dollars was allocated in the 2009-10 budget, over three years, to modernize the 77 high-risk applications. The auditor did question whether this was adequate to successfully address 77 applications. While I would have to say that more investment is always better, I would note that despite the fiscal realities, overall, MAPS was largely successful.

In fact, as the auditor noted, it remediated or retired 66 high-risk applications as of June 2016. As of today, we have remediated or upgraded an additional seven applications, for 73 in total. We continue to make progress leveraging our findings and building on the MAPS initiative.

In 2009-10, we established an application portfolio management approach, or APM. APM continues to be critical to the modernization of our systems. As noted in the auditor's report, through APM, we've established an inventory of all IT applications, and we're collecting and analyzing key data elements associated with each of those applications. Our APM approach is helping to assess each application's IT general control risk and find opportunities to rationalize and retire applications where necessary.

Our eSM division is heavily involved in this initiative and will work to mature our APM processes and guidelines. These processes and guidelines will also help establish standards for SLA creation and the better management of IT systems, starting with those classified as mission- and business-critical. Older systems do pose a challenge, especially in a constantly evolving world, where expectations and the demand for services are high. There is no question that we must continue to modernize those aging systems, but we also have to be realistic, as we are ultimately responsible for massive, complex systems of record. We need to take a balanced approach to dealing with our systems.

In order to ensure our systems are updated, sufficiently maintained and supported, we will continue to investigate long-term IT capital investment approaches for business and enterprise applications by working with program areas to understand needs and demands for service. We will proactively test and conduct threat risk assessments for our systems as part of our cybersecurity strategy. We will ensure an appropriate road map is in place for each application, to ensure they are retired or replaced at the right time.

Our approach to IT, overall, is one of continuous improvement. We have a strong foundation in place and we continue to evolve in a measured way, without putting information or security at risk.

The auditor provided recommendations that were common to three IT systems that were examined in detail: the Integrated Court Offences Network, the tax administration system and the licensing control system. Similar recommendations were made for improvements in the areas of SLAs, user access and incident problem management. I'd like to highlight our progress on those areas.

The justice, central agencies, and labour and transportation clusters have each identified targeted actions to address these audit recommendations, as outlined in the audit summary status table we submitted to the committee on May 3.

All three IT clusters are working with their respective client ministries and the eSM division to develop SLAs for the three systems audited, as well as others. They are also working to implement regular monitoring and reporting for the SLAs, which are targeted to be in place this fall. All three IT clusters are working to improve user access by reviewing access, identifying any issues, making corrections to those access levels, implementing appropriate controls to address potential conflicts and developing, most importantly, an annual user access review process. More specifically, to improve user access for the court and licensing control systems, the clusters have been working closely with their ministries to review and determine data sensitivity; to define the appropriate analytics to support user access monitoring; and to establish logging capability and reporting and develop a process for reviewing and monitoring access logs.

1250

Regarding incident and problem management for the three audited systems, it was recommended that they implement a more formal problem-management system.

This process would identify trends, the root cause of recurring issues and remediation plans for those applications.

I am really pleased to report that all three clusters are working with our eSM division to develop a formal problem-management process for all of their mission-critical applications using a consistent, approved framework. This also includes establishing a regular reporting cycle for problem management.

The recommendations for the three audited applications were very thorough. This is just a very brief synopsis of the actions we are taking to address these audit findings.

I should point out that the actions I've just noted have a designated lead within each cluster, as well as target end dates for completion. IT clusters are working very hard to ensure we are addressing the recommendations with the same level of thoroughness in order to make meaningful improvements.

As the auditor noted in her report, the IT organization supports more than 1,200 systems across government, and these systems help deliver vital services for the public, including health, education and social services. They help us manage our finances and administration, including things like making payments and collecting revenues. In fact, we process billions of transactions every year and IT is integral to doing this securely.

As with IT general controls, cybersecurity is an important component that helps ensure data confidentiality, service availability and system integrity, and as such, I'd like to briefly touch on our comprehensive approach to cybersecurity.

Many areas across the organization collaborate to identify risks. They have responsibility for ensuring the effective treatment of cyber risk and addressing threats to information assets and IT systems. Our cybersecurity operation centre operates 24 hours a day, seven days a week, every day of the year, to monitor the government's network and to respond to cyber threats or security incidents.

Cyber threats continue to evolve. For example, it is estimated that one million new pieces of malware are created every day. We address our cyber risk in a number of ways. We block almost a billion probes and scans of our network every day. We're blocking approximately 3.6 billion emails each year that may contain malicious content. And we're continuously analyzing network traffic to identify anything that may be unusual or suspicious across our networks.

We work with many internal and external partners, such as the Canadian National CIO Sub-Committee on Information Protection to ensure that issues identified anywhere across the country, whether in Ottawa or in BC, are identified to our whole community.

With increased public expectation for access to information, continuous advancements in technology and the ever-evolving threat landscape, we continue to enhance our cybersecurity posture. Having a robust, layered approach to cybersecurity is as important to me as having effective IT general controls in place, as both work together to ensure confidentiality, the integrity and availability of our IT systems.

I'm pleased to have had a chance to share the highlights of our progress on the audit. Once again, I'm committed to addressing the recommendations and driving improvement across the IT organization.

I'll turn it back to Helen.

The Chair (Mr. Ernie Hardeman): Thank you very much for your presentation. That concludes the time that was allotted for it.

We will now start the questioning with Mr. Dong.

Mr. Han Dong: Thank you very much, Deputy, and all the officials who are here attending this afternoon to give us some insight on what we're doing in IT.

To me, security is probably the most important concern. Can you tell us what your organization is doing to ensure security, as well as authorize access to government IT systems and information?

Ms. Helen Angus: I'll let David answer that, and if you want Mohammad to come up, we'll bring him.

Mr. David Nicholl: First of all, again, we thank the Auditor General for her comments and her recommendations. We agree with her comments that adequate controls are a very necessary part of defending from threats, such as hacking, viruses and the unauthorized access to information and data.

As the auditor noted in her report, our IT organization supports more than 1,200 systems across government. We're developing services for health, education and social services. We process billions of transactions across the whole gamut of our business every year, and we are extremely committed to ensuring the ongoing protection of both the privacy and the security related to any digital information held for Ontario.

Over the past 15-plus years, the technology landscape has dramatically changed. The growth in Internet usage in particular has resulted in a surge in IT-related threats. The IT organization has responded to the increased number of threats to date, and we continue to transform and put in place new measures to address these growing trends while responding to the auditor's recommendations.

To provide a sense of the magnitude of change, in the early 2000s, our IT organization's network monitoring group dealt with about two million network incidents per month and 70,000 network security events per day. Today, we have over 30 billion network security events per month and approximately one billion network security events per day. That's an increase of 15,000% in network events in the past 16 years.

Today, as I said before, it's estimated that one million new pieces of malware are being developed in someone's basement every single day. Currently, we identify and investigate around 1,400 incidents per month, and we have some reasonably serious remediation on 400 security instances every month. We've been monitoring and evolving our approach over the past 15 years to address the rapid growth in those IT threats, taking a

comprehensive, government-wide approach to cybersecurity.

An example is our response to the recent worldwide cyber attack that affected the British health care system and Germany's national railway. We've taken steps to ensure our assets and information are protected. Specifically, we analyzed the malware, which was referred to as WannaCry ransomware, and are aware it was exploiting a known vulnerability that can be addressed through the application of the Microsoft MS17-010 security patch. We deployed our security patch back in April to address this vulnerability. We deployed an updated virus scan to protect devices against this vulnerability. We communicated with OPS users to raise their awareness and to be on the lookout for suspicious emails and files. And we're in constant communication with our federal partners in Ottawa to ensure that we always have the latest information available from the federal government.

We're committed to safeguarding the data that's entrusted to us by Ontario citizens and businesses. I think we've implemented a very comprehensive approach to protecting public information and to work diligently to protect our network, information technology assets and systems against intrusions and malicious use.

Our approach to cyber risk management is holistic and risk-based, with layered levels of responsibilities to ensure the effective treatment of cyber risk. Many areas across our organization collaborate to identify those risks and have various different responsibilities for ensuring the effective treatment of cyber risk and addressing the threats to information assets and to IT systems. The organization's multi-layer approach to protecting the OPS's information assets and IT systems includes a range of corporate directives, policies, standards and tools, which include the principles for the management and use of I&IT resources, from IT directives to procurement directives.

Ministerial program areas, through their daily operations, make use of technology and systems to maintain and store information and data for both government services and the citizens of Ontario. The design, build, operation and maintenance of ministry systems are undertaken with the appropriate safeguards to meet their respective ministry confidentiality, integrity and availability requirements.

Ministries are also accountable for managing the risks related to that data. They work in partnership across other ministries and with the IT organization to ensure appropriate processes are in place.

We appreciate the auditor's comments with regard to the need to improve the security measures for our IT applications, and the IT organization will work to address her recommendations in our strategic plans over the next three years. In addition, we have an action plan to address the specific recommendations related to the three applications reviewed as part of her audit.

1300

Our cybersecurity operations area delivers cyber risk management advice and cybersecurity services across the whole IT organization. IT projects receive recommendations and support in implementing cybersecurity solutions to enable security service delivery in a digital ecosystem. This includes things like network monitoring: We have a cybersecurity operations centre operating 24/7, 365, ready to respond to any cyber threat or security incident

We have extensive vulnerability assessments and penetration testing to evaluate applications to determine their security posture and their ability to withstand attack upon request by ministries. We have threat risk assessments, where we determine the risk to IT systems, data and programs, and we recommend to ministries ways to lower those risks to acceptable levels.

We provide detailed security design advice. Probably the best time to catch security issues is when you're building a system in the first place. And we provide support to our clusters and ministries so that as they design and build solutions, they're building in the necessary security requirements for the future.

We have a range of security standards that maintain a range of policies and standards to govern the acceptable use of IT resources, all the way to technical security standards for systems design. Things like the number of bits you need for encryption on hard drives and printers—there's a GO-IT standard that, if you want to sell a printer to the Ontario government, you must meet.

Then we have education 24/7/365 awareness. Probably the most important ongoing activity that we as cybersecurity practitioners can undertake is keeping up a constant flow of learning and education towards anyone who works inside the OPS. We all know that most incidents for cyber come out of something that someone does at their desk: They open an email when they shouldn't have opened it and bad things happen. It's just through that constant education, constant learning, constant reminding of people not to do that that we protect ourselves.

The cybersecurity operations area address cyber risk in a number of ways, including analyzing all of those billions of security events in our network every day, and blocking 3.6 billion emails per year that may contain malicious content. So, literally, 3.6 billion emails that are coming into the OPS are blocked because they have the potential to contain malicious content. They're constantly analyzing network traffic and working with their partners in Ottawa to ensure that they are as up to date as possible as to: Is something strange going on? Is more traffic coming from a country? Is there something odd happening around a certain time, whether it's an election or a by-election? And, again, they're working with partners in Ottawa and other provinces, sharing information constantly and talking to each other, so they can see that if something is happening in BC, could it happen in Ontario?

The branch then also works with other strategic partners in the private sector and the federal government, really working on a committee basis to share experience, share best practices, and really try and stay on top of the next thing the bad guy is going to come up with.

With increased public expectation for access to information and the continuous advancements in technology, the landscape for cyber is just constantly changing. We really do appreciate the auditor's comments that more can and needs to be done to ensure that the continued security of information and data takes place. We are very focused on enhancing the way our security practices are delivered, and we are developing a three-year plan to drive digital resilience. We're addressing key priority areas of risk that require immediate attention. We're identifying gaps, including a strategy and road map for enhancing the operational effectiveness of the cybersecurity organization. Work is underway to move from a control-based model to a model based much more around risk. We probably cannot cover everything, but if we take a risk-based approach, we can certainly cover the high-risk areas.

Our strategic plan focuses on four key areas.

Cyber risk awareness: I spoke to that. We've got to make everybody, including everyone at this table, extremely aware of what the risks are when your email is sent to your desk. There's a risk.

We are focused very much on the risk definition: redefining risk and what the risk is, and designing answers to that risk. We want to be extremely process-driven when it comes to the treatment of the risk and the reporting on that treatment. We want to monitor and report on an ongoing basis.

Working with our partners, our plan includes proactive threat risk assessments as well as proactive penetration testing. These proactive tests would be a part of a new cybersecurity strategy for critical systems that are aging. We are currently in the process of identifying the systems and the work is under way to implement a process to proactively perform threat risk assessments and penetration testing for critical systems that are aging.

Also, we continue to evolve our approach to address threats through advanced monitoring, assessment analysis and tools such as incident monitoring tools, improved incident analysis, and training for internal cybersecurity analysts to enable them to interpret the information when analyzing incidents to help resolve incidents faster.

We want to improve application testing. We want to identify the risks, the threats, and the other vulnerabilities before applications go live or into production. We want to continuously evaluate new and emerging technologies to ensure we are deploying the best practices and technologies to protect the government's network. Recently we have seen some technology around cognitive that has that ability to tap into this network of billions of incidents that are happening every day and actually sort through so much of the noise that there is in those systems to make it vaguely intelligent to us as to what we should be doing.

Again, we really appreciate the Auditor General's comments and recommendations. They really are genuinely informing our strategy going forward. We are looking forward to having an opportunity to work with them next year and actually demonstrate what these changes have done.

Mr. Han Dong: How much time do I have, Chair?

The Chair (Mr. Ernie Hardeman): You have about five minutes.

Mr. Han Dong: Thank you very much. That was a very elaborate explanation.

Much of the auditor's report—actually, it's in a big portion of it—talked about the service-level agreements or lack of them in some respect. Can you tell us what our IT organization is doing to ensure that SLAs are applied or in place for all ministry applications going forward?

Mr. David Nicholl: Sure. As far as service-level agreements are concerned, and service management in general, we have been on a journey for a while. Probably six or seven years ago, we very much started at the hard infrastructure side of our business, which is, as we've learned from British Airways, typically where bad things can happen. We have very much focused our service management within the infrastructure.

When e-Ontario took place back in 2006-07, we actually merged and amalgamated our service management staff from the infrastructure perspective who were in clusters before. We merged them into a consolidated central organization. We really spent a lot of time very carefully sorting through the types of SLAs we wanted, what kind of reporting we wanted in those SLAs, how consistent we could make them across what at that time was a very disparate organization—much less so today.

We made our way through that process through to 2013, 2014. I think at that point we started to realize we now had the next major piece of work to do, which is from the cluster to the ministry. Again, I come back to the timing of the audit. It's perfect. It has provided really genuine insight into a rigour to implementing a consolidated and process-oriented and consistent way for clusters to administer SLAs to ministries, that on our own would probably have taken us a lot longer. We're taking a lot of actions around the SLA recommendations. We have formed our new division, enterprise service management, whose accountability it will be to actually implement the kinds of frameworks, processes and monitoring that will be required. Each cluster will be providing both formal and informal service-level agreements for each of their ministry business areas. The approach to application SLAs will be driven very much by the ministry business area. That's based very much on the approach that has been taken to date.

1310

Clearly, we have to take a much more consistent approach. By having consolidated the group responsible for doing this, we now actually can get a much more consistent, consolidated way of doing SLAs.

We certainly have SLAs in place for most of our infrastructure products today. I think we're doing well across things like our IT service desk. We're doing well on incident management. We're doing well on change management, problem management, release management—again, all from ITS, all from infrastructure out. The focus of our attention now is going to shift very much from infrastructure onto application.

I think we're taking a number of actions. Through eSM—the enterprise service management area—we are certainly looking at improving our internal and IT service delivery, we're enabling a lot more consistency in our processes for those service levels across the OPS, and we're very much looking at how that can improve the effectiveness of how we're delivering those IT services across government.

I think probably the primary duty of the new eSM—the new enterprise service management division—will be to actually enable those consistent service-level agreements across all nine IT clusters, across all 25-odd ministries, ensuring that all of the nine key elements recommended by the Auditor General are contained within each of those SLAs.

The shift on our SLAs from looking it at primarily as a hard-network, server-uptime type of operation and moving it much more into something to be a lot more realistic as to, "I'm actually getting service at my desk. Is my system working? Can I actually send a transaction?"—that's the shift we have to make now, and that's the shift the auditor really has focused on for us and has pointed out a very specific direction and methodology for us to follow.

Fred Pitt, who is here with us today, who is in charge of the enterprise service management division, is carrying the primary accountability to actually implement all nine of the pieces that the Auditor General has said.

Mr. Han Dong: Great, thank you.

The Chair (Mr. Ernie Hardeman): Thank you. We now will go to the opposition.

Ms. Lisa MacLeod: I'm just going to say a couple of things. I'm going to cede the floor to my colleague Sam Oosterhoff. This is his first experience in public accounts. He is our digital critic, and he is going to take the lead today.

I'm doing that for two reasons: (1) to make sure he gets lots of experience; and (2) I think Mr. Nicholl is probably tired of me questioning him after the gas plants scandal.

Mr. David Nicholl: No.

Ms. Lisa MacLeod: I didn't want to worry you too much today.

There you go, Sam.

Mr. Sam Oosterhoff: Perfect, excellent. Thank you.

It's very nice to be here. Thank you very much for coming in. I look forward to going through a whole bunch of questions that I have lined out.

Mr. David Nicholl: Absolutely.

Mr. Sam Oosterhoff: I was actually wondering if I could start with Robin Thompson.

Would I be able to ask you a couple of questions?

Ms. Helen Angus: Sure. Robin, why don't you come up here?

It's my first public accounts too—

Ms. Lisa MacLeod: Welcome.

Mr. Sam Oosterhoff: Okay, perfect.

Ms. Helen Angus: We can be novices together.

Mr. Sam Oosterhoff: Excellent. That's the way to be.

Mr. David Nicholl: We're the experts, obviously.

Laughter.

Ms. Helen Angus: I'm sort of a slow learner.

There we go. Robin, the floor is yours.

Ms. Robin Thompson: Thank you. Hello, I'm Robin Thompson. I'm the chief information officer for the justice cluster.

Mr. Sam Oosterhoff: Perfect. So why is it taking the justice IT cluster so much longer to implement these changes, given that you have less services than the other two clusters?

Ms. Robin Thompson: If I could ask for a little bit of clarity on which services. Are we speaking of SLAs or—could you give me just a little bit more clarity?

Mr. Sam Oosterhoff: Right. A user access review procedure, which has been taking longer at the justice technology services cluster, compared to the other two clusters, given that the justice cluster has less systems to support than the other two.

Ms. Robin Thompson: The justice cluster has 106 mission-critical, business-critical solutions. The focus of this audit for general controls, as you know, focused on our ICON system. We have dug into our user access and appropriate security permissions that we have in there.

We do have a current formalized process whereby staff are submitting electronic forms, and they are requiring appropriate manager approvals. The forms that we produce indicate appropriate system access and update capability for permissions. Our service desk works in conjunction with us for tracking and assigning the work. We review for accuracy and appropriateness, and our management approvals are matched to the update capabilities within the requests we receive.

Mr. Sam Oosterhoff: Perfect. So do the other two clusters do all that as well?

Ms. Robin Thompson: I would ask my colleagues to comment on their processes in their own systems. This is something we took quite seriously from the audit, actually, and we do have processes today that are already in place for user control and security access.

Where we found the gap to be is in the documentation of these. The group of ministries, the justice sector, is a very tried and true organization. As part of the onboarding of people, the processes are very clearly communicated, but they are communicated across multiple areas. We need to strengthen our documentation of that in a central repository where people could access that documented process.

But the rigour to ensure that people receive the right security access, and that user IDs are set up with the right permissions, does exist today. It is in an electronic fashion, with multiple levels of approval.

Mr. Sam Oosterhoff: I think it's very, very important, as my colleague MPP Dong mentioned, to maintain that security, right? That's something that's so fundamental.

At the same time, I'm just curious. Why would less systems that you're working on—perhaps David can speak to this: why you believe the justice cluster is taking

that much longer. Is it more complicated, or are the other people not doing due justice—I didn't mean that as a pun—

Mr. David Nicholl: It's pretty good.

Mr. Sam Oosterhoff: But could you explain?

Mr. David Nicholl: Anywhere we start seeing variations across the nine clusters—typically, if you kind of scrape the top of it off, you said it, there's probably going be a complexity reason in there somewhere as to why one application has found it easier, perhaps, to undertake a change or an improvement than others. It usually comes down to a complexity issue, either technology complexity—or maybe not. Maybe it's just business complexity: How many people are using it? How many different divisions within a ministry are using it? How many other parts of government use that application for some other reason?

If you look at the drivers' database, for instance, it's used by pretty much everybody in government. It's probably the most used database we have. So it raises the complexity when it comes to any kind of service management activity around those applications, whereas, if you've got a fairly straightforward, stand-alone, five-person-use only, one-function application, it will likely be easier to do. So my guess would be, if we went and looked under the covers of the complexity of what Robin is maintaining—and I know this—it is hugely complex.

Mr. Sam Oosterhoff: Perfect. All right. I was curious about that.

David, back to you, then: We spoke about the aging systems and what that looks like, and how aging isn't always necessarily a bad thing. I would agree.

Ms. Helen Angus: So would I.

Mr. David Nicholl: So would I.

Mr. Sam Oosterhoff: But the reality is that some of these platforms are from over 40 years ago. I'm curious what the interprovincial standard is, where we fall into that, and what your plan is going forward as we see a lot more cloud-based computing and a lot more tech that's built in that sort of concept, where we don't have the traditional platforms the way—I mean, we're using a Commodore 64 when we could be using an iPhone 7. I'd love to hear your thoughts on that and what you believe we need to do going forward.

Mr. David Nicholl: Great question. We've recently, actually, done some work around comparing ourselves to market. We undertook a fairly exhaustive 12-month exercise in different numbers of varieties of things, of checking things, and one was age. When we compare ourselves to a typical public sector organization of our size and complexity, from an average perspective, we come out just shy of what the average is. So we're slightly younger, but the average really is kind of irrelevant. It's the out ones that are really going to catch you. You're absolutely right: We have got some wonderfully mature—I like to call them—applications and they are quite often the workhorses of any organization. This is not by any means a government comment. I did 20-odd years in banking. I can guarantee you that our personal accounting systems in our major banks are just as mature as some of our systems are in government. They have to be because they are—some people call them your crown jewels. They are literally holding the data that drives so much, whether it's a bank or whether it's a government, forward.

1320

I think what the Auditor General said very, very clearly in her audit is, "Look, if you can modernize, great. Obviously that's a good thing, but if you can't, there are some things you need to be quite concerned about." I think one of the things that the Auditor General really focused on was people, how we are ensuring that, for some of these systems, we have the people in place who can continue to maintain them.

Between us clusters, we actually have a very good system of almost emergency bells going off when we have some of the older technologies that are failing, and people will come together almost as a centre of excellence. Like, "Who knows their way around an IMS DC environment?", and you'll get four or five people putting their hands up, certainly someone in Wynnann's area—I see you put some nice thing at the end here—who can help. There are always a few people around you who can actually do this. We do that. We make sure, from a people perspective, that even though the full-time team isn't there, there's somewhere else they can go to get help, if necessary, typically backed up by a vendor—typically.

Most of our older technologies are IBM technologies and IBM still will retain knowledge. They will still be licensing these products. They will still be maintaining these products, but there's no doubt it's getting harder, and that is absolutely a point well taken from what the Auditor General has said. I think I mentioned in my response that we're very keen to really jazz up our IT capital planning piece where we can actually, just as roads and bridges do, start talking in the same language as roads and bridges: "Are we replacing? Are we replenishing? How much money should be put into that system? Is it worth to maintain it?"

Mr. Sam Oosterhoff: I agree. I'm just curious. You can only maintain something for so long, right? What do you think that's going to look like going forward? I was actually very curious about the cloud-based—

Mr. David Nicholl: Yes.

Ms. Helen Angus: Will you talk about the cloud?

Mr. David Nicholl: Sure.

Ms. Helen Angus: Because we've got a really, I think, prudent but active agenda to move into the cloud. So we can talk about the recent procurement—

Mr. David Nicholl: Yes, totally. Certainly on the RUS side, which is the drives and vehicle side where some of our more long-in-the-tooth applications are, I think we've got a very careful plan to actually take us off some of those older applications, and moving some of those systems into the cloud may well form part of that strategy.

We're well into the cloud now. We've been careful with it, I think, for extremely good reasons. We, frankly,

have been waiting for industry to come to Canada, to be quite honest. It has taken them a while, but we've seen, in the last 12 months, really 12 to 24 months, that the major cloud providers—and that literally is Microsoft, Google and AWS. That's it. They are the major, major—I hope IBM isn't listening. They are the three major hyper cloud providers today. We are already working with AWS. We run Ontario.ca, a public-facing website, within AWS. We're doing some work within Microsoft Azure, and, really, as application opportunities come along for replacement, if there's a software-as-a-service opportunity, we'll take it first—absolutely take it first.

We have probably two or three major SaaS programs running today. Our procurement system that we run in the OPS is a pure SaaS product, Bravo. Our learning management product that we run across all the OPS is a pure SaaS product. Our hunting and fishing licences system that we run is a pure SaaS product. So there are a few that—we've cut our teeth on it, but there's no question, with the Canadian content of the hyper-providers of cloud, that it will absolutely open up more opportunities for us going forward, for sure.

Mr. Sam Oosterhoff: Perfect. That actually touches on something you mentioned earlier: That in banking you hold large amounts of important data, and also in government, obviously. You mentioned earlier that you work with Ottawa and you work with other partners. I was curious: Do you work with CSEC, and what does that look like when it comes to monitoring some of the—

Mr. David Nicholl: My Ottawa man will come to the table.

Mr. Sam Oosterhoff: The million pieces of malware a day is a stat that a lot of people are thinking of, especially after the ransomware attacks, right?

Mr. David Nicholl: Yes, absolutely.

Mr. Mohammad Qureshi: My name is Mohammad Qureshi. I'm the head of cybersecurity operations for the OPS. When we talk about working with our federal partners and working with our jurisdictional partners within the provinces, there are a couple of avenues we go through. One of them is that we are part of the NSC coalition, which is the national subcommittee for CIOs on information protection, where all of the chief information security officers or heads of cybersecurity meet once a month to share intel around threats that they may be seeing. For example, when Vancouver was going through the general election just last month, we were seeing some malicious activity around that, and they were making sure we were aware of that. We were actually protecting our network around that.

The other piece we have is that we're in direct contact with our federal intelligence agencies—CSEC, CCIRC and CSIS—to receive intel. An example I can give is the WannaCry global ransomware threat that we just experienced not too long ago. We had already patched our systems for that vulnerability well ahead of the WannaCry ransomware issue, but at the same time, as soon as that started propagating around systems, we were receiving intel from our federal government partners to ensure that we had indicated a compromise, that we were actually implementing blocks around our government network.

Mr. Sam Oosterhoff: Perfect. On that note of cybersecurity, that was almost more specific malicious security from outsider nations or hostiles or however you want to put it. But what about—perhaps not maliciously, but they're working on the job—one of those 41% of users who had access to the system when their job status does not require any access at all? I know you went into a little bit of detail, but for me it sounded like what you were saying was such common sense that I can't believe you weren't doing it before. I'd love to hear a bit more about some of the steps that you're going to be taking to address what I think is one of the most important aspects of this, that users are granted inappropriate access to sensitive and confidential data.

Mr. Mohammad Qureshi: There are a couple of things I just want to highlight at a general level that address that point. One of them is that there's a layered approach to identity and access management that we take. When we look at employees onboarding with the OPS, for example, we follow HR processes to onboard them. As part of that, program area managers are actually reviewing the individual who is being hired. They're actually filling out access forms to get completed detailing requirements for access to systems, the level of access required and the role that they're going to be playing. Once the request is submitted, the I&IT organization will create the active directory account, and that gives them access to the OPS network. That's one layer around it.

The next piece is, depending on the system that they're accessing and the level of sensitivity of information held in that system, there is a level-of-assurance process that we go through, and it's typically assigned through our PKI certificates. Depending on the level of sensitivity of that information, that employee will have to go through a fairly rigourous ID proofing process to ensure that they are who they say they are before that PKI certificate is issued to them. Once that PKI certificate is issued, then the I&IT clusters will actually onboard them to the specific application, doing access control with that system.

The other example I like to give is that once an OPS employee does leave the organization, the program area manager will complete a request to terminate that employee. Once that employee is terminated in our HR system, the PKI certificate is automatically deactivated, to ensure that they don't have access to that system, and the active directory account is also disabled. So if the employee doesn't have access to our government network, they can't get access to the system that they had access to. The other piece that David spoke about earlier is that all of the I&IT cluster CIOs are now also implementing routine reviews of that access list.

1330

Mr. Sam Oosterhoff: Okay, neat. Since we're talking about the people and the HR perspective, one of the

things that struck me was that you're not following best practices in computer management, such as programmers entering actual data into the court system, which could result in programmers inadvertently or fraudulently entering inaccurate data or altering existing data.

What would you say are some of the ways to move forward to change that? One of the concerns with this is that innovation that could improve service delivery was not occurring because of this, so I would love to hear what we can do to improve this—from a security perspective, as well.

Mr. Mohammad Qureshi: There are two things I would like to comment on. One is, can I ask the specific application you may be referring to in the audit? But while you're looking for that, the one thing I would like to say is that we routinely invest in technologies within the cybersecurity operations branch to leverage new and upcoming technologies.

The one example I will give is that within our cybersecurity operations branch, we do use user behaviour analytics and artificial intelligence to highlight anomalies that people may not be normally doing to trigger an investigation that we would have to take a look at in a deeper fashion.

Interjections.

Mr. Sam Oosterhoff: I apologize. Would you be willing to repeat the last, like, minute's worth?

Mr. Mohammad Qureshi: Sure, not a problem, absolutely. The one thing I was going to say at an enterprise level from the cybersecurity operations branch is that we do invest in technologies that leverage user behaviour analytics, as well as artificial intelligence, to analyze network traffic within the government of Ontario network. When David mentioned that we analyze 30 billion, it's almost close to 40 billion network security events per month now with some of the later technologies that we've implemented. That starts highlighting deviations from normal patterns that users may be doing.

If we look at insider threats, which is a big issue within the cybersecurity realm, it's typically looking at behaviours around a large volume of data leaving an organization. That would trigger an incident or an alert within our cybersecurity operations centre to actually start triggering an investigation around that.

Mr. Sam Oosterhoff: Right, but that's not specifically the example of what could happen where programmers would inadvertently or fraudulently be actually entering data into the court system themselves. What you're saying is that when people extract large amounts of data, alarm bells go off, but if people are putting in fraudulent data, there's no real way to figure that out? It just sort of happens?

Ms. Helen Angus: Maybe Robin can answer that, because of her role and relationship to that specific system.

Ms. Robin Thompson: Thank you for the opportunity. This particular item was something that took a lot of my attention in the report back from the audit, actually, because it is very important that we implement best practice. It also relates to the size of teams in maintaining systems and making sure that there's an appropriate segregation of duties, but at the same time making sure that we maintain system stability and making sure that the data is appropriately updated.

There are a few things that I would like to comment on in this area, because I agree that best practice is incredibly important—

The Chair (Mr. Ernie Hardeman): That may have to be in the answer to the next question, because that time is gone, and we're now going to the third party.

Mr. Taras Natyshak: Are we doing two rounds?

Interjection: Yes.

Mr. Taras Natyshak: Oh, we are? Okay. That's fine.

Thank you very much for being here. Thanks for informing us. You're sort of the guardians of the galaxy when it comes to data, and that's very cool. My questions are, I think, pretty pointed, so bear with me. They may not be as elaborate as my colleagues', but it's just stuff that I want to learn.

Why would an agency not enter into a service-level agreement at the point of purchase with a vendor? Why would they choose not to? Why would we have such a gap?

Mr. David Nicholl: I think the real emphasis is on the formality of what the agreement is. Whenever you buy something from anybody, there's always a level of agreement between the purchaser and the seller. I think what this is all about is bringing a rigour to what that agreement is. We have been lax in the rigour and the formality of what should go into that agreement. That's what the Auditor General really focused in on.

You know what an SLA is; there are lots and lots of informal SLAs between clusters and ministries. Everyone knows, if a system goes down, when it should come back up, but what's missing is the formality of an agreement between the two parties and, I think most importantly, actually a follow-up and reporting on how you're doing against those targets. That's the key part. It's the formality and the reporting that's important.

Mr. Taras Natyshak: Is the goal now, then, 100% coverage of SLA?

Mr. David Nicholl: Yes, but we'll do it by risk order.

Mr. Taras Natyshak: Does that mean that there will be a higher cost incurred to your department or to those various departments? Does an SLA mean that that agreement costs more?

Mr. David Nicholl: No. I think our evidence has been—when we did this back in 2006-07 on the infrastructure side, we had driven costs down within the infrastructure organization very much because we now have a consistent, enterprise-wide way of doing certain things and measuring certain things and it's not being done in nine or 10 different ways across the organization. It doesn't have to cost any more money, absolutely not.

Mr. Taras Natyshak: Okay. Great answer, by the way. I'm sure the government will be happy to hear that.

Was the last major application review in 2010, or has there been another one? Just through listening to your

submission, I believe, Mr. Nicholl, in 2010, the budget was $600 million for 77 applications to remediate or upgrade.

Mr. David Nicholl: Yes. So the last effort to go forward with a consolidated ask for money for a number of applications was in 2010.

Mr. Taras Natyshak: When will you do that again?

Mr. David Nicholl: Well, this is the discussion that we had coming out of the audit, that I think there is interest in us putting together—whether it's MAPS II or not, I don't know, but certainly to take a look at how we can look at IT application modernization, just the exact same way as we look at road and bridge modernization. In theory, it shouldn't be any different, so the onus is on us, working with Treasury Board, to actually come forward with a capital plan for all of these applications based on risk, based on need, based on, potentially, age: Where should government focus its investment dollars?

Mr. Taras Natyshak: Thank you.

In your answer to Mr. Dong's question on security, your follow-up within your statement, if I caught it correctly, said, "We will proactively test" for cybersecurity risks, inferring that it's something that you're going to be doing. I would imagine, and I've heard, that it's something that is an ongoing thing. Was that just—

Mr. David Nicholl: We do it on an ongoing and frequent basis. Mohammad can probably answer this better. I would say it's probably not 100% consistent, and I think what we want to do, again, to come back to the consistency question, is make it a consistent exercise. Is that fair?

Mr. Mohammad Qureshi: Absolutely. And I can add just a little bit to that. We do perform threat risk assessments and penetration testing to systems today. On average, we probably do anywhere between 120 and 150 threat risk assessments to systems every year.

The comment that Mr. Nicholl made was more around how we start doing more proactive pen-tests and threat risk assessments to aging systems. It's just formalizing the risks around those aging systems and actually doing those more proactively than is being done today.

Ms. Helen Angus: We also now do that as a regular course. As a former deputy of international trade, any time anybody leaves the country, we actually do have a formal process to look at the opportunities for cybersecurity and making sure that anybody travelling for the government of Ontario is fully aware of the risks and understands what they need to do to safeguard against those. Those vary depending on the jurisdiction of travel. So that's now imbedded in our travel request process.

Mr. Taras Natyshak: We should pass this information over to Donald Trump and give him some tips on how to protect cybersecurity and his exposure to those threats. So it sounds like we're doing well there.

1340

So, CSOC: That's Cyber Security—

Mr. David Nicholl: Operations Centre.

Mr. Taras Natyshak: —Operations Centre, 24/7. Have any of the investigations that have come out of that resulted in any formal criminal investigations? And, if any, have any charges ever been laid?

Mr. Mohammad Qureshi: So, as far as I've been in the role, I am not aware of any criminal investigations or criminal charges that have been laid. The majority of the incidents we see that require investigation and remediation are typically malware or ransomware: Someone receives an email that wasn't blocked at our perimeter, clicks on the attachment or clicks on the link and gets their hard drive encrypted, similar to what happened with WannaCry. What we do is we sort of isolate that computer, reimage it, do an investigation and then we issue a new computer to the user.

Mr. Taras Natyshak: So working in conjunction with our partners at the federal level that have that shared jurisdiction, you're not aware of any further investigations on their part that they've taken? I guess I would want to know that if we were able to track where these threats are coming from and actually pinpoint who is doing it—at some point it would be nice to level the full extent of our laws onto them and ensure that there's a deterrent out there for those attacks to stop.

Mr. Mohammad Qureshi: Absolutely. What we do is that whenever we do see incidents, we share our indicators of compromise back with the federal level, so with CCIRC. We will share with them what we saw and where the traffic was coming from, and then it sort of goes into that intelligence world of trying to identify and pinpoint exactly where that was coming from. When it comes to that world, I don't know if I would be at liberty to really speak openly around what those investigations may be.

Mr. Taras Natyshak: On recommendation 2 from the AG's report: In reference to the ICON program, overall the response or the completed undertaking is that—

Interjection.

Mr. Taras Natyshak: Sorry, Chair, my mike's way over there. The SLA for the court system has been developed. Overall, 12 SLAs are now signed off, of 94. How long for the remainder of those 94? How long would you anticipate that taking?

Ms. Robin Thompson: Thanks for the question and the opportunity to give you an update. Our original agreement, as you noted, from 2007 was what we referred to as a general service-management framework. That was an overall relationship on how we would interact, between the justice cluster and the business, but it really created sort of a separation. That operating agreement has since been transitioned into the detailed SLAs, as you say.

We have completed the SLA now for ICON. It is finished. It contains the nine commitments that were recommended within the audit. Also, we have successfully been able to review the details of the agreement with our business colleagues. We have obtained their approval and sign-off, are now going into operation and will be starting the reporting process on that imminently. In addition, we have focused significantly on this with our operations team, and we now have 70 mission- and

business-critical and business-support SLAs drafted. The drafts are complete, and 27 of them, as of today, have been reviewed and approved by ministry business partners.

Mr. Taras Natyshak: So you're on your way.

Ms. Robin Thompson: We took the agreements very seriously and put them into action, because we are using the standard template that we have in the cluster for now and will transition, and we are using the nine elements.

Mr. Taras Natyshak: Making it easier for you. Very good.

How much time?

The Chair (Mr. Ernie Hardeman): You have about 16 minutes left.

Mr. Taras Natyshak: I have 16 minutes left?

The Chair (Mr. Ernie Hardeman): Oh, no, it's about 12 minutes.

Mr. Taras Natyshak: Oh, that's great. I thought time was going by quicker than that. I'm sorry.

Mr. Bob Delaney: Only when you're having fun, Taras.

Mr. Taras Natyshak: That's right.

Recommendation number 1 of the AG's report: For SLAs for all applications, number 3 is that your response or the Treasury Board's response is to "ensure regular reporting to ministries on the performance of mission and business critical applications compared to the expected performance." The simple question is, how regular is this reporting? Is there a formal format that you're going to undertake?

Mr. David Nicholl: It'll be monthly.

Mr. Taras Natyshak: Monthly? Okay.

Mr. David Nicholl: They committed to monthly.

Mr. Taras Natyshak: Okay, we'll hold you to that. I would imagine that that's a good interval to continue to provide oversight and collaboration, as well.

Ms. Helen Angus: Once you have the metrics and you can start to pull the data, it becomes fairly easy to populate on a monthly basis, so you get into a system of doing it regularly.

Mr. Taras Natyshak: Okay. Some of my other questions—I think I only have a couple more. The office of the corporate CIO didn't have an inventory of all I&IT applications prior to the AG's report. Why not? How come? How did we not know exactly what was out there?

Mr. David Nicholl: You know, it's one of those things that you want but you never quite get to the end of. We actually started this exercise probably—Wynnann, when did we start doing our inventory? Two years ago?

We had done it prior to MAPS, because we really needed that very strict inventory of what was there, and then we go out of the way of keeping it updated. So it had been there. It got out of maintenance mode, and a couple of years ago we really kicked in again and said that we really wanted to make sure that this was solid.

One of our reasons for doing it was that we actually had a target to reduce the number of applications we run, because we were north of 2,000 back 10 years ago, I guess it was. We had a target saying that we really want to get that number down through retirements and all of the various ways you do that.

We did a recent count. Wynnann led it, and we're down to—how many?

Ms. Wynnann Rose: It's 1,351.

Mr. David Nicholl: It's 1,351 applications now.

Mr. Taras Natyshak: So 1,351 applications that—I'm thinking of applications in this sense. Is that okay to think of them as that?

Mr. David Nicholl: Yes, meaningful, not a spreadsheet.

Mr. Taras Natyshak: Okay, not a spreadsheet. A function of a system?

Mr. David Nicholl: Yes, it's doing something useful.

Mr. Taras Natyshak: Yes. And some of those applications are vendor-based?

Mr. David Nicholl: Yes.

Mr. Taras Natyshak: Some are not?

Mr. David Nicholl: Correct.

Mr. Taras Natyshak: Some are developed in-house?

Mr. David Nicholl: Yes.

Mr. Taras Natyshak: Some are on a fee-for-service type of—what is it?

Mr. David Nicholl: SaaS? Software as a service?

Mr. Taras Natyshak: Yes.

Mr. David Nicholl: Very few, though.

Mr. Taras Natyshak: Very few?

Mr. David Nicholl: Very, very few.

Mr. Taras Natyshak: Are we paying for applications that aren't in use? Are there applications that have been orphaned, that are no longer required, that are obsolete, that we're still paying for? Has that audit been done?

Mr. David Nicholl: That audit is being done, because we now have a current and maintained inventory of every application we have.

Mr. Taras Natyshak: Now we do, so now we can do it?

Mr. David Nicholl: Now we do. For clusters, we have a very interesting savings initiative going on that the Treasury Board is leading and that I&IT is a big part of. We have our own so-called "boulder," which is our transformational savings target. One of the lines in that is actually application rationalization, so we are targeting anywhere we can find an application that's doing things like correspondence applications, for instance, where we may have two or three across the OPS where one would do. We are going after those to choose which one we're going to have: Do we get rid of all three and shut them down, or have one? It's rationalizing our application portfolio. We've been doing this for 10 years. We haven't finished.

Mr. Taras Natyshak: Do applications that are provided through the SaaS model present a particular vulnerability, either in assessing their function or their vulnerability to security risks? I'm thinking of MNR systems that exist in the States, where data is housed in the States. Is that a consideration?

Mr. David Nicholl: It's absolutely a consideration. It's something that we took very seriously with the IPC at

the time. Prior to awarding that contract, we had a fairly intensive dialogue with Dr. Ann Cavoukian, who at the time was the Information and Privacy Commissioner, to ensure that our contracts that we wrote were the right contracts to make sure that both privacy and security were an integral part. We reserve the right to audit and to check up on them, to make sure that what they say they are doing they are doing. With that specific vendor, they're a very targeted vendor who just do that piece of business. They're not a generalist at all. So they're a very tight-run operation we feel very good with.

1350

On the cloud side, in general—I forget whether it's just software as a service, but anywhere with the cloud—the rigour that we're now involved in as far as writing those contracts is extensive. The IPC, again, has issued a pretty long and detailed set of guidelines around what should be in a contract for a cloud provider. We are following that very, very closely. Any time we look at a cloud service, we work very closely with the IPC from a privacy perspective. We work very closely with Mohammad's people, and then Mohammad's greater empire, into the private sector, Ottawa, and all the various places that are looking at this, to ensure that the kinds of rigour and surety we need as a government are being met. So we can look Ontarians in the eye and say, "Your data is as secure as we can possibly make it." That really is our guideline.

Mr. Taras Natyshak: You mentioned that cyber-risk awareness is something that you're embarked on with employees who interact with systems across all ministries. Are you telling me that people are still opening emails from Saudi princes who want to give away their fortune?

Mr. David Nicholl: You know, it's not the Saudi princes anymore and it's not the Nigerian people giving away money. There was one yesterday—

Ms. Helen Angus: I sent it.

Mr. David Nicholl: I know you did. We got one yesterday; it's good. You may have got it. It's an e-fax notification and it's from a genuine e-faxing company that says, "You've got a fax and you should click on to get your fax." Your natural inclination is to just go click on the fax, and it's spam.

Mr. Sam Oosterhoff: It happens right away.

Ms. Helen Angus: I've been trained, so my nose was twitching. I said, "I don't think I should open this." I regularly send David, or probably Mohammad, emails that get through that screen, and have them open them. Then they tell me, "No, don't open it. Delete it right away" or every now and then it's actually okay. But this one was really hard to identify.

Mr. Mohammad Qureshi: The one thing I would like to add is those emails are getting more and more sophisticated, and a lot of the attackers are using more and more socially engineered approaches trying to attack, right? A lot of times people will do research on your Facebook accounts, your LinkedIn and your social networking accounts that are already opened. They will target messages directed to you, so you feel like it's a legitimate message coming through. Very seldom do we see those Saudi princes sending out those emails anymore.

Mr. David Nicholl: It's targeted; it is so targeted.

Mr. Taras Natyshak: Thank you for your time. Thanks for the work that you do, and thanks for presenting and being here today.

Mr. David Nicholl: Thank you.

Ms. Helen Angus: We appreciate the questions.

The Chair (Mr. Ernie Hardeman): Thank you very much. We'll now start the second round with the government. Each party will have 17 minutes in this round. Mr. Dong?

Mr. Han Dong: Thank you, Chair. It's a very interesting topic. I'm glad that we're not going to see many Saudi prince emails anymore.

But the work you do, I want to make sure that you get the credit for it. It's a very tough, challenging environment, because it changes so fast. And with all these social media means out there, new things are popping up all the time.

I consider myself, given the nature of my work, tapping into the latest tool. But you always see new things come out. Almost every six months there's something hip.

From some perspectives, you have a very cool job. You guys are considered as cool dudes out there in the cyber-world.

I heard the mentioning of the ICON system. Can you tell us a bit more about that? What does it do? What are we doing with it, and stuff?

Ms. Robin Thompson: Sure. Thanks for the question. The ICON system is a case-management and tracking system for both adult and youth for provincial offences. It supports the act and the matters from that for the Ontario Court of Justice. It has scheduling and it has financial reporting. It's a very robust and large system. It is 27 years old. It is a large and stable mainframe system that we have, supporting over 5,000 users today. It is one of our significant, mission-critical systems that we have within the justice sector. It's an integral part of our criminal system, and processes information through the courts.

We are very concerned about and have put a lot of effort into the stability and ongoing operation of ICON, as we refer to it, as our brain or, really, our integral system. We have upgraded our hardware, our software, our operating systems and our ability to print remotely around the province, to ensure we maintain operational stability.

One of the observations that I had when I came to the justice cluster was the incredible focus that the cluster folks had on operational stability. Very, very rarely do those systems fail. ICON is one of those systems. It is capable—and continues today—of processing thousands of transactions on a regular basis, and is really the system of record that people are accessing and using every day.

We have modernization strategies within both the cluster and the ministry now, which will see us eventual-

ly replacing ICON and modernizing those systems. The detailed planning for that is happening next year, in 2018.

In the interim, we are developing smaller systems and digital technologies to increase the integration of information, which also accesses ICON and takes information out and in.

Also, we are implementing self-service capabilities as well, for people to generate work that they would normally have to come into the courts to do, and then people would enter it manually into ICON.

There's a lot of exciting work happening right now within the justice system.

Mr. Han Dong: That's great. The auditor's report mentioned the government spending on I&IT in the last 10 years as being somewhat steady or unchanged. I'm just wondering what we are doing to maintain efficiency or maybe control the growth of expenditures on this.

Ms. Helen Angus: I'll let David answer that. I think he has already used the word "boulder," which is kind of the language that we use at Treasury Board to describe clusters of activities and how we look at their budgets. The I&IT organization has been a focus of that work.

Mr. Han Dong: It's not easy, because on the one hand, you have all the technical advancements, and a growing population and the growing needs and challenges, and expansion of government programs and services. On the other hand, how do we take advantage of technology and make sure we can—

Ms. Helen Angus: Yes. David can describe, a little bit, what we've done on the application side.

Maybe you can talk also a little bit about what we've done on the people side as well, because we've achieved some savings in the I&IT organization, so we're pretty happy about that.

Mr. Han Dong: That's great.

Ms. Helen Angus: Do you want to dig into it?

Mr. David Nicholl: Sure, happy to. Absolutely. We ran a pretty interesting benchmarking exercise a few years back, just to give us a better idea as to what our spend really was, against comparative jurisdictions. We came out about 10% below average, when it came to our spending.

It's done on a fairly rigourous method of functional point analysis. There's an ability to count quantitatively what makes up one of those 1,300 applications, basically. It's how much logic, how many reports, how many screens—there's a way of counting to decompose an application into a number of function points.

We've got a pretty good idea—we've got a very good idea, in fact—of what the complexities of those applications are, and how much we're paying for it. That means we can compare ourselves across other jurisdictions.

We came out about 10% lower. We're not a top-quartile performer. We're above average, so it gives us that opportunity, I think, to push ourselves into that top-quartile performer.

1400

How did we get there? We got there through the work we just talked about earlier. The 2008-09 consolidation that we did on infrastructure really was the beginnings of really driving into an efficiency of the stuff that you just need to make things work. It's the commodity types of business that we run. Whether that is running a data centre, running a server, a network or running an e-mail account, those things are commodities: things that we should be able to drive the price really down to rock bottom. We do a lot of them and therefore we can get very efficient data.

We have spent, I would say, the last nine years really focused on driving the cost of the commodity-based services to as low as it possibly can go. There are a few areas that we're still focused on and we run these exercises pretty constantly to make sure we know where we are on the efficiency line. We know we're good when it comes to that commodity-type service.

The reason for doing that is—and you're quite right; you've noticed that the IT spend since about 2003 has been reasonably flat. We went through an accounting switch, because I think we all used to be cash and now we're cash and capital. You have to be careful about comparing numbers across. Generally speaking, we're within a reasonable boundary, I suspect, of same spend. But what we've done is we've dramatically changed where it's spent. We've really driven down as much as we can that spending on commodity-type services and we continue to push that. The boulder that Helen mentioned—a big chunk of our next $100 million savings target, which we're getting through well—is still focused on the commodity-style pricing. That means that we go after vendors with a vengeance, typically. I hope they're not listening. We really do try and—

Mr. Han Dong: Well, it is on the record.

Ms. Helen Angus: They probably have real experience with that.

Mr. David Nicholl: We work our contracts very competitively. We look for innovation in our contracts where vendors perhaps are at a point in time where they would like to do something with you and we extract maximum value. I would say if you look at our contracts with people like, on the hardware side, IBM, Oracle, HP, we're very good at managing those contracts and we manage them well.

The important thing on it is we've shifted the spending from that sort of commodity—not terribly interesting work—into clusters. Clusters are where the business end is really focused on. It's where innovation takes place. It's where our ministries and our businesses are focused on how we can make better services for Ontarians, make better services for businesses, how we can do things more efficiently, how we can make sure that cheques get out on time. That's where we want to spend the money we're spending, not on the commodities side.

I think, just generally speaking, we have spent nine years, and we will be spending another two or three through the end of this boulder exercise, focused on driving out unnecessary spending within the IT budget and actually pushing it into the discretionary spending area on business solutions.

We're pretty proud of (a) holding our spend, but (b) not only holding our spend but actually shifting it from commodity to value add. That's what we want to do.

Mr. Han Dong: Good to know. Thank you. Can you tell us more about the licensing control system and what we're doing to address the findings by the auditor and perhaps modernization of that system?

Mr. David Nicholl: I know Wynnann Rose would be delighted to come up and talk to you about the licence control system.

Mr. Han Dong: Please introduce yourself.

Ms. Wynnann Rose: Hi, I'm Wynnann Rose. I'm the CIO for the Ministry of Transportation and the Ministry of Labour—the labour and transportation IT club. Thanks for the question and the opportunity to talk about the licensing and control system. It really is the workhorse, the heartbeat of the Ministry of Transportation.

The licensing and control system, or LCS, is comprised of five subsystems that enable the Ministry of Transportation to license and register drivers, vehicles, carriers—which is trucks and buses that travel along our highways—and provide oversight for the motor vehicle inspection stations, the MVIS.

The system manages over nine million drivers, over 12 million vehicles, over 57,000 carriers, trucking companies and bus companies, and 13,000 motor vehicle inspection stations. These systems are particularly important to the MTO because they allow us to support the annual non-tax revenue of $1.7 billion into the ministry.

As well, there are many stakeholders that access these systems, as you can imagine. Everyone in the province is interested in having access to drivers' information, including law enforcement, courts, insurance companies, the municipalities, the 407, etc. The list goes on. There are about 50 different stakeholders that require access to that information.

The labour and transportation cluster agrees with the Auditor General's recommendations. We are a very proud ministry, a very proud IT organization. We do what we think is great work, but the recommendations were received in a way that allows us to continue to move forward. We have, of course, improvements that we can be making.

The steps that we've taken for improvement, based on the auditor's recommendation, include updating our service-level agreements. There was kind of a lengthy discussion about that. We have implemented the service-level agreements according to the Auditor General's recommendations and we have, as of the middle of May, signed off 90 of the service-level agreements for our applications, including the licensing and control system, which is the most mission-critical of our solutions at MTO.

We're moving forward using the same template, the same process, to implement these SLAs across the rest of the ministries and the other divisions of the ministry. We're working with our partners in the enterprise service management team to begin to report on those SLAs and metrics and, once we have those metrics, to work to improve the service if required.

On the user access issues that were identified, or opportunities that were identified with the licensing and control system, we obviously recognize the importance of effective controls on user access and monitoring and logging of access to the system, as the data is extremely sensitive and critical to the ministry.

Logging of user access is something that's been in place for many years in the ministry. It is a process that's very rigourous and mature. Anyone who is accessing our systems in the ministry for drivers, vehicles and carriers goes through a process where they are vetted by their manager or an authorized approver to have access to those systems. We log who is using the system in an inventory and we also have built-in tools within the system that log all access.

Those logs, at the time of the audit, were not organized in a way that there was easy access to the logs. Since the time of the audit, we have pulled out all the log information and we have a system now that does historical reporting on who's had access to the system. As you can imagine, it's a very busy system and the database that holds the log files is 3.6 billion records. To sort through that and understand who is having access to those business transactions is now made a lot easier for ourselves, as well as internal audit or FOI requests.

We're also, based on the recommendations, working with the ministry to improve the review of our user-access control. We have done, based on our internal audit reports, many reviews of that access, but in the last 12 months there have been two formal reviews, and we put in place documentation to allow us to do an annual review, regardless of any kind of periodic review that we want to do.

Right now we're looking at stale records. We're working with ServiceOntario, who is one of the main users of this system, to go through and remove any stale users who haven't accessed the system in over 60 days. That work is coming to a close in June.

1410

I just want to emphasize that the ministry and officials always understand who has access to our systems. It is logged and maintained by the ministry, as well as the IT organization.

In addition to that, we are implementing new business intelligence dashboards, hopefully working with our colleagues in cybersecurity, to pull all this information out about who's accessing our system and which transactions they're using and putting it into real-time dashboards so that we don't only have an historical look at who's accessed the system, but we can monitor it in real time and allow us to be a little more proactive in understanding who's accessing the systems.

The Chair (Mr. Ernie Hardeman): That may be a very good place to say thank you very much for that answer. We'll now go to the official opposition: Mr. Oosterhoff.

Mr. Sam Oosterhoff: One of the things that actually stuck out to me right at the end, because it's going back to what I was talking about before about the access

issues—I know we've thrown the ball around the room a couple of times now, but you mentioned that you always have knowledge of who has access to everything, essentially. Is that what you said? Two minutes ago you said, "I want to be very clear that we always know who has access to our files."

Ms. Wynnann Rose: We know who has approved access to our systems.

Mr. Sam Oosterhoff: Right, approved access.

Ms. Wynnann Rose: Yes.

Mr. Sam Oosterhoff: If you always know who has access, then how come there's still that amount of people who would be able to access it who don't need to access it, that 41% number, going back to that? I know that was in a different ministry, but within all three IT systems, users were granted inappropriate access to sensitive and confidential data. We talked about that. But if you always know who's accessing everything, then how are they still doing that?

Ms. Wynnann Rose: The way the user access control works at the Ministry of Transportation—it's a very mature process that's been in place within the ministry for many years; as long as I've worked there. People request access to these systems using proper forms. There are only certain groups of authorized approvers who can approve that. Those forms come in, they're accompanied by a security check and they're accompanied by someone signing off—

Mr. Sam Oosterhoff: Maybe I asked the wrong question, then. Maybe I'm just confused. Could you clarify, because I think I'm maybe getting mixed signals. On the one hand, you're saying pretty much no one can access it because it's very difficult, you have to go through all this process—

Ms. Wynnann Rose: A very rigourous process.

Mr. Sam Oosterhoff: Very rigourous, but then, on the other hand, it says with all three IT systems users are granted inappropriate access to sensitive and confidential data. There seems to be something that contradicts, unless I'm not seeing something right. You're the security one, right, the cybersecurity one?

Mr. Mohammad Qureshi: Yes.

Mr. Sam Oosterhoff: Sorry.

Mr. Mohammad Qureshi: No, it's okay.

Mr. Sam Oosterhoff: Would you be willing to speak to that briefly?

Mr. Mohammad Qureshi: Sure. I can revert back to the whole process of onboarding and off-boarding staff to ensure that when people do gain access to it, there's a very rigourous process to ensure that they have access to the system and that they are who they say they are. Right?

So if I go back to talk to how we onboard employees to the OPS and the layered approach to identity and access management that we take, once the program area manager approves that this person is allowed to access this information, they're being hired into a specific role, the program area manager will submit paperwork and that kicks off our IT process around providing the user with an active directory account, which just allows them to access our government of Ontario network. Then, depending on the level of sensitivity of information—if there's a system of record that has very highly sensitive data in it, they have to go through a level of assurance process, and the higher the sensitivity that data might be, the more rigourous that process is, all the way through to getting background checks and making sure that the ID they provide to us—we can physically validate that ID by looking at that person, looking at their ID and then also validating that ID in a system of record, like the driver's licence system.

Mr. Sam Oosterhoff: Before I lose my train of thought, Auditor, wasn't there something about how the audit said that they didn't have proper definitions of what critical information was or that there wasn't—how do you define what critical and confidential information is? When does something become critical, when is it not, and how do you determine those?

Mr. Mohammad Qureshi: We have an information sensitivity classification policy that defines what the level of sensitivity of information is. The higher the sensitivity is, the more chance that it could cause harm, fraud and other things defined within that policy.

When we do our threat risk assessments, we use that information sensitivity classification policy to work with the program areas to identify the level of sensitivity that information has. Based on that sensitivity level, we actually apply controls from a security perspective and provide recommendations back to the program area on how to reduce risks that may be highlighted through a project.

Mr. Sam Oosterhoff: I'm kind of switching gears, David, to the court system. So much of what I'm hearing is that a lot of this is just human error when things are going wrong—because it seems to be a few things.

One of the curious things that I read in the summary was that "in January 2016 the system went down temporarily … and was unavailable for front-line staff because multiple programmers had been working on making changes to the code at the same time, without knowing each other was doing so."

Within the audit, it speaks about how "even if the Ministry of Justice was able to find people who know the programming language of the system, there would be a significant problem because the documentation they would need to perform their duties is incomplete, outdated or, in some cases, non-existent."

This kind of boggles my mind, because I know some friends who are in the civil service—they're very dedicated—and they all talk a lot about documentation and how important having that paper trail is. When I was first elected, I had two different friends come up to me and go, "Make sure you keep note of everything, because that's what we've been taught in the public service"—

Mr. David Nicholl: Everything.

Mr. Sam Oosterhoff: Everything. I'm just curious: How did that come to be a significant problem, where there is a lack of documentation and you have two people

working on making changes to the code at the same time without even knowing about it?

Ms. Robin Thompson: Do you want me to—

Mr. David Nicholl: Yes, sure. I would do it from a purely general level, but if you want to talk about ICON, go ahead.

Ms. Robin Thompson: Actually, I'm happy to have this, because it's a follow-on from the conversation that we started prior. I think it has a lot to do with segregation of duties that you're referring to and also about the appropriate job responsibilities and how they're documented.

If I could start and then progress from there, based on what it is that you're wanting to know.

Mr. Sam Oosterhoff: Sure.

Ms. Robin Thompson: The first thing, unfortunately, that I do have to say is that I do not have knowledge of a January 2016 occurrence of this. We proceduralize, actually, and I receive updates from my operations team whenever there is an outage to a mission-critical system. Then I'm actually talking to deputies' offices to ensure that we have it. I would have to follow up on that for you. I apologize; I cannot comment on that right now.

Mr. Sam Oosterhoff: That's okay.

Ms. Robin Thompson: However, having said that, you mentioned several other items.

If I understood properly, one item would be that our developers have clearly articulated roles and responsibilities and document it. One thing I will absolutely confirm is that all of our employees, including our developers who work on the court systems, have specific job responsibilities that are documented. They have particularly what their jobs entail—job descriptions, if you will; sorry, I was searching for the correct terminology. It's very clear what their jobs and their roles are.

When we go into your previous question, which is again the two developers at the same time, I would have to follow up on that for you, because I do not have knowledge that that has occurred or that it occurs on a regular basis. Having said that—

Mr. Sam Oosterhoff: I hope not.

Ms. Robin Thompson: I would agree. It's very important to have best practices and have the right complement of people looking after your systems, which was another observation, because of ICON's duration and the direction in which we think we still have to go before we modernize it.

Talking about segregation of duties, we do have the case, and had the case, which was of great interest to me where we have our developers occasionally—that has also been validated—making changes into the production system. However, these changes are by no means done ad hoc. They are initiated from the courts with management approval, go through an electronic form submission as a service request, and then, as they come in, they are fixing data, specifically on the traceability, to sign that off.

1420

Having said that, that is not optimal. It's not optimal to have your developers who develop actually going into the production database, I would agree with you, for best practice. So we've made some changes. With the ministry, we're partnering to conduct a review of all the security access, including a full review of the appropriate segregation of roles and responsibilities related to system permissions, who is granted to do what and what changes they are able to make under any condition that we have.

As I said, it's important to tell you that all of these data update requests are very infrequent and are coming to us from documented formal service requests. However, in the interim, until this entire review and until we can make the appropriate changes—also, as we're augmenting our team, because that will create more capacity—we are going to make a change, by the end of June, actually, that all update requests will now be routed to the JTS operational support manager for a case-by-case assessment for service continuity impacts on court operation. Data updates in the production system will therefore only be implemented on an exception basis, where there is a confirmed service continuity impact, and with the authorization and documented approval of the manager in JTS and the manager in courts, with full traceability of the change.

We also have system logging, which would capture that change, at the ID level—

Mr. Sam Oosterhoff: Perfect.

Ms. Robin Thompson: So that is an interim change.

Mr. Sam Oosterhoff: Okay. Just because I have a couple of other questions I want to get to—

Ms. Robin Thompson: Sure.

Mr. Sam Oosterhoff: Sorry about that. I appreciate it. I'd love to continue at more length some other time.

One of the other things in the court system is that there is the situation where all programming changes in the court system are currently being made by two individuals—one staff member and one consultant, who is not under supervision—but there is no succession plan. I'm just curious. If we have this drastically changing technology and we have aging technology—IBM is not really supporting us anymore, from what I've heard—what sort of succession plans are you acting on to improve that situation? Because that is concerning—if someone gets into a car accident and unfortunately doesn't make it—

Ms. Robin Thompson: Agreed.

Mr. Sam Oosterhoff: You know, situations arise.

Ms. Robin Thompson: The first thing I would say is that I want to reiterate that continuity of operations and properly trained people is a priority. ICON is very stable, yet it uses dated technologies and is programmed in an older mainframe language. However, the age of the system is not a direct indicator of reliability.

We in the cluster maintain, operate and support the application of ICON, and we work in partnership with our other areas to support the operating platforms. To ensure the sustainability of our systems, we've updated the hardware, the operating system and the database software, as well as the environment which facilitates the printing capability across all the provincial courts. They've all been updated as recently as 2016. I am very

confident that the system continues to be robust. It continues to be able to process thousands of transactions.

Mr. Sam Oosterhoff: Right. The system—yes. I'm just curious about what sort of impact that would have if one of those two people—

Ms. Robin Thompson: Okay, so let's talk about the people.

Mr. Sam Oosterhoff: Right? It's more the HR perspective.

Ms. Robin Thompson: Absolutely. No problem.

Since the audit, we've increased our ICON support capacity, and now we are current; we have the right-sized team and skills to support the team.

Mr. Sam Oosterhoff: Perfect. That's exactly what I wanted.

Ms. Robin Thompson: Okay. So here's our strategy: Our strategy is to supplement our permanent employee complement with contracted skill sets, because they're still available in the marketplace. When you combine the skill of the internal employees—so you've got that stability and you have the ability to transfer from one person to another—we're able to balance the need to sustain and implement ministry changes, which we still do, and also plan for the modernization of ICON. It's important to have that balance between employee and contracted resources.

We've now hired an additional development contractor, for a total of two, plus our permanent developer that we have. We're also in the process of recruiting another position to the ICON team to ensure that we maintain a continuous approach to succession planning, instead of reactive.

We now have an additional dedicated support employee—a business analyst—responsible for change requirements and the design, working with our business, as well as doing application testing in a more formal way.

Finally, we have a technical support resource for the ICON database administration, a DBA.

These resources that I just mentioned are incremental to the three that were mentioned in addition to the contracted resource in the audit. They were our ICON helpdesk representatives, and they are still there, but they have a very separate function: to field calls, track incidents and try to resolve issues as they come.

Mr. Sam Oosterhoff: Thank you very much. I appreciate that.

Ms. Robin Thompson: You're welcome.

Mr. Sam Oosterhoff: I know I keep picking on the court system.

Ms. Robin Thompson: That's okay. Even though it's my first time here, go ahead.

Mr. Sam Oosterhoff: That makes two of us.

If we go back to the money aspect of it—because obviously, unfortunately, from this government we've seen a lot of, in my opinion and I think in a lot of Ontarians' opinions, misallocation of resources or misspent funds or mismanagement. When I look at the court system, where $11 million was initially spent with the goal of replacing the system as part of a much larger IT project, they wrote off $4.5 million on that plan. Although the court system and licensing system were flagged as overdue for replacement and modernization under MAPS in 2009 and 2010, they haven't been replaced or modernized.

I know you spoke about this briefly, but I'd love to hear a little bit more about what that modernization plan is, going forward. You mentioned the allocation for three years, but we still haven't actually seen the completion of that project. What do you think the future is going to hold? And how do you think the auditor's recommendations will help you in that role as you work forward with that?

Ms. Robin Thompson: I need a little help to break that down. That was many questions in one question.

Mr. Sam Oosterhoff: I apologize.

Ms. Robin Thompson: I need you to break it down into things you want me to answer for you, and I will.

Mr. Sam Oosterhoff: For sure. After $4.5 million being spent on an initial project, nothing has been replaced or modernized in the court system or licensing system even though that was given in MAPS in 2009 and 2010. Could you speak about that and then about how the auditor's recommendations will allow you to improve on this going forward—or will, hopefully, force you to improve on this going forward?

Ms. Robin Thompson: The audit focused on general controls. Those would be the checks and balances within systems. So they would ensure that we have traceability, continuity and proper procedures that adhere to the directives and our policies. When we talk about why we have not modernized ICON or what's happening with the modernization agenda, and also that we had a previous project whereby there was $4 million that was not able to be "repurposed," for lack of a better word—there have been previous plans and projects focused to replace ICON and modernize the criminal justice system. However, the scope of the project has been very ambitious and has proved too complex to implement. The Court Information Management System, the CIMS project, is the project you're talking about when you're talking about the money.

The Chair (Mr. Ernie Hardeman): You can blame the shortness of the answer on the length of the question, but the time is up.

We'll go to the third party.

Ms. Robin Thompson: That always happens to us. I'm sorry about that.

Mr. Sam Oosterhoff: Rats. We just have a good relationship. We'll talk.

The Chair (Mr. Ernie Hardeman): Taras?

Mr. Taras Natyshak: I simply want to give the remainder of the time—however much you want to take—for you to inform us, as members, as to what your needs are, or on any challenges that might lie ahead that weren't identified in the AG's report.

Also, the dreaded "what do you know that you don't know" question: What is it that is on the horizon that you don't know exists but we should still be prepared for?

Ms. Helen Angus: Actually, this is a pretty interesting part of the Treasury Board portfolio—not for the issues around controls, but just for the opportunity that I&IT can play in the transformation and the betterment of public services.

I'm quite excited about the work that David is doing around using the cloud, looking at how we can use I&IT to help us collaborate differently within the public sector to provide better advice and work more horizontally than vertically, because I think it really allows us to do that. I'm quite anxious to see that work move at a clip that would allow us to tackle some of the more complex issues and problems facing the province, and do it in an innovative way.

1430

We've also hired, as you probably know, a chief digital officer, so the idea of having, in addition to this team, a team that's really focused on working a little bit more iteratively with my team, starting to think about how we can do digital first for the end users, the people of Ontario, as a means to access information or conduct business with the government of Ontario—that's a pretty big agenda to move on all at once. That's kind of keeping the pressure on. Being able to meet the expectations of providing services differently, I think, is part of the challenge that lies ahead for us.

You may have a different perspective—

Mr. David Nicholl: No, no—never different, Helen.

Just a few other things that I'd say: I'm sure lots of people come here and give the auditor all kinds of kudos for helping them with their jobs, and I'm sure she takes it with a large pinch of salt at times. But I think, in this case, and we met early on, the timing of this audit was tremendously important for us, because we were about to embark on this consolidation of service management, in the non-traditional sense, in that we were really good at the infrastructure of service management. Email accounts, desktops and helpdesks—we were good at that. But the much harder world we're in is business solutions. That's where it's really difficult. The 1,300 applications—that's where CIOs have such a really, really tough job.

I think you can help us by supporting some of the really positive actions that an audit can take to help us do our jobs better. It's not just all about perhaps trying to find something that we're not doing well, but in this case, it's really been about, "Here's a road map of something really useful for you guys for the next couple of years. You'll come out of that and it's just going to be better." That's genuine. I may say it anyway, but in this case, it really is very, very genuine.

Ms. Helen Angus: I think some of it has to do with the skill of the audit team that was actually deployed and having the experience in IT.

Mr. David Nicholl: It was a super team—a really, really good team.

Ms. Helen Angus: That really made a difference. It was incredibly helpful to have that knowledge base within the audit team. It was terrific.

Mr. David Nicholl: So a great question: "What should you be worrying about?" In other words, what do we not know about that you don't know about. I think we've had a very brief, slim discussion on cybersecurity here. We should be under no thoughts whatsoever that we are not—we will be attacked and we will be compromised at some point. Anyone that doesn't think we will be is living in a dream world. We will. Mohammad and his team are focused entirely on trying to protect us. But in fairness, all it takes is one employee to double-click on an attachment in an email, and we could have issues.

I think the three-pronged attack on cyber with the planning piece—and that goes to education: "Don't open that email." How can we make sure our CSOC is operating? All of that pre-work we're so focused on, because that's non-discretionary work. We've got to do that. That's just table stakes.

When we get hit, we have to really know what to do, and it would be interesting to start thinking about how we extend that. We had a very interesting tabletop exercise last week, where we went through a true-life incident concerning a cybersecurity breach in the Ontario government. It was on a piece of paper on a table, and it was a complete eye-opener for us as to what kind of shape we were in during an attack when data was being taken, ransoms were being held and we had to make tough decisions. I think that area of what happens when you actually are attacked, when it's happened and you're under a ransom situation, we have to have the process down pat, because it's not the time to make decisions when you're in that circumstance.

I think the third piece of it, then, that generally we probably don't talk enough about is, and then, what afterwards? How do we actually recover from an incident, where perhaps Ontarians' data has been compromised? We have to be ready for that circumstance.

I think that just the recognition that we certainly, the two of us, live in this world of just assuming we'll lose one day and someone is going to get us, we have to be ready for that situation and ready to react.

That probably is not something that we talk a lot about, but that's what really keeps us awake at night. We'll do everything we can to protect, but we also have to realize that there are so many bad guys out there who are—if you're doing something that they're interested in in the House or you're passing an act or you're discussing a topic and somebody might want to know about it, you just don't know. It could well become that. I think that's a very interesting part.

I think you can help us a lot by just keeping an eye on what perhaps isn't as important as some other things. It's very simple in the technology world for people to get distracted by what the next new, shiny object is. Sometimes, that can cause all of us to go into a difficult freezing moment of what the heck are we going to do now?

I think that just a level of common sense—we are a government; we're here to serve the people of Ontario

and their business. We probably don't need to be all things to all people all the time. I think just keeping an eye on that is probably a really useful function you can do for us as well.

Mr. Taras Natyshak: Very good. Thanks for the work that you do and thanks for being here today.

Mr. David Nicholl: Not at all. Thank you.

The Chair (Mr. Ernie Hardeman): On behalf of the committee, we want to say thank you for being here this afternoon and helping us out with this review. It's great that you've taken to the fact that I have to keep cutting people off because the time is out. We do appreciate your participation. Thank you very much.

Ms. Helen Angus: Thank you. Thank you for your questions and your requests. We really appreciate that.

Mr. David Nicholl: Thank you very much.

The Chair (Mr. Ernie Hardeman): With that, before the committee rushes off, we'll go to legal personnel for a short period of time to discuss with legislative research as to what we'll do with the report-writing.

Thank you very much. We'll wrap.

The committee continued in closed session at 1437.

STANDING COMMITTEE ON PUBLIC ACCOUNTS

Chair / Président
Mr. Ernie Hardeman (Oxford PC)

Vice-Chair / Vice-Présidente
Ms. Lisa MacLeod (Nepean–Carleton PC)

Mr. Bob Delaney (Mississauga–Streetsville L)
Mr. Vic Dhillon (Brampton West / Brampton-Ouest L)
Mr. Han Dong (Trinity–Spadina L)
Mr. John Fraser (Ottawa South L)
Mr. Ernie Hardeman (Oxford PC)
Mr. Percy Hatfield (Windsor–Tecumseh ND)
Mr. Randy Hillier (Lanark–Frontenac–Lennox and Addington PC)
Mr. Monte Kwinter (York Centre / York-Centre L)
Ms. Lisa MacLeod (Nepean–Carleton PC)

Substitutions / Membres remplaçants
Mr. Taras Natyshak (Essex ND)
Mr. Sam Oosterhoff (Niagara West–Glanbrook / Niagara-Ouest–Glanbrook PC)
Ms. Lisa M. Thompson (Huron–Bruce PC)

Also taking part / Autres participants et participantes
Ms. Bonnie Lysyk, Auditor General

Clerk / Greffier
Mr. Katch Koch

Staff / Personnel
Mr. Ian Morris, research officer,
Research Services